U.S. Department
of Transportation

**Federal Transit
Administration**

Sensitive Security Information (SSI): Designation, Markings, and Control

Resource Document for Transit Agencies

FTA

Federal Transit
Administration

March 2009

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The United States Government does not endorse products of manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average one hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE March 2009	3. REPORT TYPE AND DATES COVERED

4. TITLE AND SUBTITLE Sensitive Security Information (SSI): Designation, Markings, and Control, Resource Document for Transit Agencies	5. FUNDING NUMBERS
6. AUTHOR(S) Kevin Chandler,* Pamela Sutherland,* Donald Eldredge*	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) *Battelle, 505 King Avenue Columbus, OH 43201	8. PERFORMING ORGANIZATION REPORT NUMBER CG005580
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Office of Safety and Security Federal Transit Administration 1200 New Jersey Ave, S.E. Washington, D.C. 20590	10. SPONSORING/ MONITORING AGENCY REPORT NUMBER
11. SUPPLEMENTARY NOTES	
12a. DISTRIBUTION/AVAILABILITY STATEMENT No Restrictions. Available From: National Technical Information Service/NTIS, Springfield, Virginia, 22161. Phone 703.605.6000, Fax 703.605.6900, Email [orders@ntis.fedworld.gov]	12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

This document includes resource information for identification and handling of information pertaining to transit systems and transit operations whose dissemination should be controlled and protected for security reasons through the use of designating this information as Sensitive Security Information (SSI).

14. SUBJECT TERMS Sensitive Security Information, SSI, Transit Agency, Security	15. NUMBER OF PAGES 32
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT None

ACKNOWLEDGMENTS

This resource document was originally developed for the Federal Transit Administration's (FTA's) Security and Emergency Management Technical Assistance Program (SEMTAP) by Battelle, including staff from Transportation Resource Associates (TRA) and Total Security. The document was finalized as part of the FTA's Office of Safety and Security strategic planning program.

The authors wish to acknowledge the input and leadership of Rick Gerhart from FTA's Office of Program Management's Office of Safety & Security.

The authors would also like to acknowledge FTA's Office of Program Management and Office of Chief Counsel; the U.S. DOT's Office of the Secretary's Office of Intelligence, Security and Emergency Response; FTA's All-Hazards Strategic Planning Team, the Transportation Security Administration (TSA); the American Public Transportation Association (APTA); the Transportation Research Board (TRB); and numerous transit agencies for their input in the development of this resource document.

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS

CCTV	closed-circuit television
CD	compact disc
CEO	chief executive officer
CFR	Code of Federal Regulations
CUI	controlled unclassified information
DHS	U.S. Department of Homeland Security
DOT	U.S. Department of Transportation
DVD	digital versatile device, also digital video disk
FAA	Federal Aviation Administration
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FR	Federal Register
FTA	Federal Transit Administration
HTUA	high-threat urban areas
IT	information technology
LES	law enforcement sensitive
PC	personal computer
PCII	protected critical infrastructure information
SSI	sensitive security information
SBU	sensitive but unclassified
TSA	Transportation Security Administration
USC	United States Code
VPN	virtual private network

1. Scope and Purpose

This guidance document addresses sensitive security information (SSI) for transit agencies.

Sensitive security information (SSI) is information about security, operations, facilities, or other assets or capital projects whose disclosure would be detrimental to the security of transit employees or customers.[1] By law, transit agencies are required to categorize and protect SSI. Protecting SSI means restricting its distribution and controlling access to it. By law, SSI is not subject to disclosure under the Freedom of Information Act (FOIA)[2] or state "Sunshine Laws."[3] It is also not available under discovery in civil litigation, and it is not required to be part of the record in a federal rulemaking.

The Federal Transit Administration (FTA) has based the guidance in this document on the regulations in 49 Code of Federal Regulations (CFR) Parts 15 and 1520. Its purpose is to help transit agencies prevent the unauthorized disclosure or dissemination of SSI while preserving the public's "right to know" about transit systems and operations.

Transit agencies can use this guidance as a resource in developing policies and procedures for identifying, marking, and handling SSI in order to control access to it. To the extent practical, agencies should integrate the designation, marking, and handling of SSI into their existing security procedures.

---

[1] SSI is defined in 49 CFR § 15.5 as "…information obtained or developed in the conduct of security activities, including research and development, the disclosure of which the Secretary of DOT has determined would—
(1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file;
(2) Reveal trade secrets or privileged or confidential information obtained from any person; or
(3) Be detrimental to transportation safety."

[2] Title 5 United States Code (USC) § 552

[3] "Sunshine Laws" are statutory laws based on the idea of "openness" in government, with public access to records and meetings and the conduct and activities of government.

2. Background

SSI was created by the U.S. Congress in 1974 as part of a response to a wave of airline hijackings. Initially, SSI was limited to the aviation industry. After September 11, 2001, however, the designation of SSI was extended to include all modes of transportation through regulations in 49 CFR Parts 15[4] and 1520,[5] both titled "Protection of Sensitive Security Information." Specifically, in February 2002, the Department of Transportation (DOT) transferred the responsibility for protecting SSI from the Federal Aviation Administration (FAA) to the new Transportation Security Administration (TSA),[6] then a part of DOT. In May 2004, TSA issued an Interim Final Rule that extended SSI protections to all modes of transportation.[7]

Since May 2004, TSA has amended the Interim Final Rule several times. These amendments resulted in minor changes to several definitions and descriptions. As the TSA introduces new security-related regulations for transportation, the definitions and descriptions in the SSI regulation will continue to change. The most current versions of these regulations are available at the following websites:

- Code of Federal Regulations – http://ecfr.gpoaccess.gov/
- Federal Register – http://www.gpoaccess.gov/fr/index.html.

[4] 49 CFR Part 15 applies to agencies regulated by the U.S. Department of Transportation (DOT).
[5] 49 CFR Part 1520 applies to agencies regulated by the U.S. Department of Homeland Security (DHS).
[6] 67 Federal Register (FR) 8351, February 22, 2002.
[7] 69 FR 28066, May 18, 2004.

3. Categories of Protected Information

The Federal government designates several categories of protected information. Security-related information can have a designation of "classified" or "controlled unclassified information." **Classified** national security information is information designated by executive order whose improper disclosure could result in harm to the national defense or foreign relations of the United States. Classified information is categorized as confidential, secret, or top secret. **Controlled unclassified information** (CUI), formerly **sensitive but unclassified** (SBU) information, is not classified but has limits on public disclosure. Categories of CUI include:

- Sensitive security information (SSI)
- Protected critical infrastructure information (PCII)
- For official use only (FOUO) information
- Law-enforcement sensitive (LES) information.

This guidance document addresses only SSI. If transit agencies combine SSI with other types of sensitive but unclassified information, they must mark the resulting information as SSI.

Sensitive security information (SSI)

For transit, SSI is any information or record whose disclosure may compromise the security of the traveling public, transit employees, or transit infrastructure. SSI may include data, documents, engineering drawings and specifications, and other records whose disclosure could increase the agency's risk of harm. For example, threat and vulnerability assessments are SSI.

SSI requires protection from public disclosure as defined under FOIA[8]—that is, SSI is not subject to disclosure either under FOIA or state "Sunshine Laws" and, by regulation, it *must not* be disclosed. Failure to categorize or mark information as SSI does not change its protected status.

Protected critical infrastructure information (PCII)

PCII is information related to critical infrastructures or protected systems—that is, PCII is not customarily in the public domain.[9] It includes information about actual, potential, or threatened interference, attack, compromise, or incapacitation of critical infrastructures or protected systems, and the ability of critical infrastructures or protected systems to resist such interference, compromise, or incapacitation. Transit agencies may come in contact with PCII through interaction with the Federal government.

For official use only (FOUO)

FOUO is a designation used by some Federal agencies to protect sensitive information from public release. Unlike SSI, however, FOUO information is not exempt under FOIA.

---

[8] FOIA exemption (b) (3) covers information "specifically exempted from disclosure by statute (other than section 552b of this title) provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld."

[9] For a complete definition of PCII, see 6 CFR §29.2.

Law enforcement sensitive (LES)

LES is a designation used in law enforcement to protect information related to active investigations. LES information has a specific exemption under FOIA, but, depending on interpretation, may ultimately be releasable under FOIA. Distribution of LES is limited to law enforcement officials. Only transit agencies that have law enforcement units should encounter this category of sensitive but unclassified information.

4. Types and Forms of Sensitive Security Information (SSI)

Types of SSI

By regulation, SSI currently includes 16 types of records.[10] At this time, only the types listed below apply to transit agencies: [11]

1. Security programs and contingency plans issued, established, required, received, or approved by DOT or DHS

2. Vulnerability assessments that are directed, created, held, funded, or approved by DOT or DHS, or that will be provided to either agency in support of a Federal security program

3. Threat information held by the Federal government concerning transportation, transportation systems, and cyber infrastructure, including sources and methods used to gather or develop the information.

Transit agencies must categorize, mark, and control these types of records as SSI. In addition, the TSA Administrator and the Secretary of the DOT have the discretion to determine that other information not listed above is SSI.

Transit agencies in high-threat urban areas (HTUA)[12] may possess all three types of SSI listed above as well as come into contact with SSI designated by the TSA Administrator or the Secretary of the DOT. Smaller transit agencies and agencies in rural areas may not have a need to possess or come in contact with any SSI. Transit agencies possessing any of these records must categorize, mark, and control them as SSI. Failure to mark records as SSI does not change their status as SSI.

In addition to the types of records listed above, transit agencies should evaluate the following to determine if they are SSI or contain SSI.

- Security program plans and procedures that include vulnerability records or specific tactics for security operations[13]
- Security contingency plans and records
- Records that reveal system or facility vulnerabilities (e.g., maps, detailed facility drawings, detailed action items from drills and exercises)

---

[10] 49 CFR §15.3 and 49 CFR §1520.3 define a record as "any means by which information is preserved, irrespective of format, including a book, paper, drawing, map recording, tape, film, photograph, machine-readable material, and any information stored in an electronic format. The term record also includes any draft, proposed, or recommended change to any record."

[11] For a complete description of the 16 types of SSI, see 49 CFR §1520.5, Sensitive security information

[12] HTUAs are typically larger-population metropolitan areas with a relatively high concentration of critical infrastructure or operations.

[13] Many security plans place this type of information in an appendix that can be separated from the rest of the document. If the appendix is redacted from the document, the remainder of the plan is not SSI and can be distributed as needed to a wide range of audiences.

- Information about threats against the transit agency or other local transportation.

Forms of SSI

SSI may include both printed and electronic records such as letters, memoranda, reports, plans, procedures, illustrations, tables, graphs, and drawings; blueprints, schematics, maps, and charts; photographs, negatives, and unprocessed film; slides and transparencies; films and videotapes; microfilm and microfiche; and audio recordings.

Electronic records may include magnetic tapes, floppy disks and diskettes, compact discs (CDs), digital versatile devices (DVDs), hard disks, removable media, disk cartridges, optical disks, paper tape, magnetic cards, tape cassettes, and other forms/formats of information where the information that are removable from the electronic system by the user or operator.

SSI may also include information distributed via the Intranet and Internet, such as e-mails and text messages.

5. Identifying and Designating SSI

SSI designation is based on regulations in 49 CFR Parts 15 and 1520. Sections 15.5 and 1520.5 define SSI as follows:

> "...SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which the Secretary of DOT has determined would—
> (1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file;
> (2) Reveal trade secrets or privileged or confidential information obtained from any person; or
> (3) Be detrimental to transportation safety."[14]

All transit agencies that accept grant money from FTA or DHS must determine if any records that they possess meet the definition of SSI and must categorize, mark, and control them.

Some information provided to transit agencies, for example from the TSA or FTA, may already be categorized and marked as SSI. However, for internally generated records, transit agencies need policies and procedures for identifying, marking, and handling SSI that comply with regulatory requirements.

Any transit agency employees who would reasonably be expected to create records that might contain SSI should be able to evaluate those records for potential SSI content. If a record potentially contains SSI, the employee should refer it to a designated employee or committee responsible for making SSI determinations.

Identifying SSI

To determine whether information could be SSI, transit agency employees should consider the threat environment within their operating areas and around their facilities and infrastructure as well as the following:

- Does the public need to know this information? For example, for safety reasons, transit agencies must share emergency evacuation and response plans with a wide audience. Categorizing such information as SSI could discourage its distribution.

- Is the same or similar information readily available from other sources? For example, the location of a closed-circuit television (CCTV) camera that is in plain sight in a transit facility is not SSI, whereas a map showing the locations of all CCTV cameras in a transit system might be SSI.

- Could someone intent on causing harm misuse the information? For example, could someone use it to target facilities or operations? Does the information

[14] 49 CFR Part 15 applies to safety and Part 1520 applies to security.

increase the attractiveness of a target or place transit agency infrastructure or operations at greater risk of threats?

Table 1 provides examples of records that might be SSI and records that usually are not SSI.

Categorizing records as SSI

Transit agencies can best maintain public confidence by providing complete and accurate information in a timely manner and assuring that only information requiring security protection is categorized as SSI. Categorizing too many records as SSI may needlessly increase operational costs as well as make access to the records unnecessarily difficult. Information on controlling access to SSI is provided later in this document.

The general managers/chief executive officers (CEOs) and the chief counsels at transit agencies should be involved in selecting experienced employees or committees of experienced employees to formally identify and categorize records as SSI. These individuals or committees might include employees from operations, information technology (IT), executive management, security, safety, engineering, facilities maintenance, and legal, and may also include individuals from local or regional FTA and TSA offices. As appropriate, the committees or individuals may be congruent or overlap with the committees or individuals that handle security breaches at the transit agencies.

General principles that individuals and committees can use for identifying whether records should be categorized as SSI include:

- Base identification of SSI on the regulatory definition and types of SSI listed in 49 CFR Parts 15 and 1520.
- Do not categorize as SSI information relating to the environment, safety, or health unless security requirements significantly outweigh the public's need to know.
- Do not categorize records as SSI out of convenience or a desire to keep them private.
- Do not use SSI to conceal or delay the discovery of regulatory violations, errors, or inefficiencies; to avoid embarrassment; or to restrain competition.
- Categorize records as SSI only if record-holders can be notified of the categorization, and the SSI can be uniformly protected. The individual or committee making the designation is responsible for notifying holders.

If only a portion of a document is SSI, transit agencies must categorize and control the entire document as SSI. To release the document, transit agencies must first redact the SSI from it.

Initially, the individuals or committees selected to categorize records as SSI should review and evaluate all transit records that could potentially be categorized as one of the "Types of SSI" discussed in Section 4 above. In addition, prior to releasing any records in response to litigation or public request, the committees should review the records to determine if they contain SSI.

Transit agencies should also periodically review their policies and procedures for identifying and designating SSI to assure compliance with regulations and to identify records.

Table 1. Examples of SSI and Non-SSI

Might Be SSI	Usually Not SSI
System Design and Operational Information	
Transit system design configurations, including architectural drawings and engineering schematics; critical assets and network topology maps; exposed, unattended, or unprotected assets; critical infrastructure layouts; energy sources; and communications assets and procedures	Environmental, safety, or health information.
Installation and design-related operational information concerning critical equipment or components that, if sabotaged, could prevent operation or safe shutdown	Information needed to comply with laws and regulations
Security System Design and Equipment Information	
Records of vulnerabilities or security deficiencies at specified facilities or locations, or within the transit agency in general	Information discernable by casual observation
Records of specific locations and design or operational details of internal security devices, such as sensors, detectors, alarms, and barriers	Budgeting and cost information
Information about the capabilities and limitations of security systems, and methods and times to defeat or degrade equipment, operations, or mitigations	General information about equipment
Security procedures and operations that are of a non-routine nature	Routine administrative data
Information about physical security vulnerabilities and deficiencies, especially if they have not been corrected	Records of past facility and equipment evaluations that do not reveal security-related deficiencies or that reveal deficiencies that have been corrected
Information about intrusion detection, alarm, or assessment equipment, including physical and cybersecurity plans and performance of installed equipment	Installation records for intrusion detection, alarm, or assessment systems
Information about security system design or integration, including heightened-risk operating procedures	Commercial vendor information about security equipment and systems
Data on security personnel assigned to specific transit facilities, including times and locations, where information can not be determined by casual observation	Total number of security personnel assigned to transit system facilities, or the fact that personnel numbers are being increased or decreased
Emergency and Emergency Communications Information	
Some emergency procedures, including heightened-risk operating procedures, contingency plans, and business continuity plans	Fire response and evacuation plans that must be shared with all employees
Records of assessments, drills, or exercises that reveal system or security vulnerabilities	Records of communications equipment used by transit authorities, including emergency management
Ridership Data	
	Information about the number of passengers on individual trains or buses or at a particular time of day

6. Marking SSI

SSI records require a protective marking and a distribution limitation statement to inform users of their security-sensitive nature and the need to protect them from unauthorized distribution as defined in 49 CFR §15.13 and §1520.13.

SSI records in both printed and electronic form must be marked as follows:

SENSITIVE SECURITY INFORMATION

and must include the distribution limitation statement specified in the regulation:

Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

For paper SSI records, the protective marking must appear at the top of every page, including the outside front and back covers, binder covers, and title pages; and the distribution limitation statement must be at the bottom of every page, including the outside front and back covers, binder covers, and title pages. The protective marking should be printed or stamped in a font size larger than the text of the record. Electronic documents must be similarly marked and the distribution limitation statement included on every page. Appendix A contains sample front and back-cover pages for paper or electronic SSI.

For non-paper SSI records such as videotape and audio recordings, the protective marking and the distribution limitation statement must appear clearly and conspicuously on the record so that the viewer or listener is reasonably likely to see or hear them. In addition, non-paper SSI records should be kept in containers that are clearly marked on the outside.

Floppy disks, CDs, DVDs, tapes, and other media on which electronic SSI is stored should also be marked, either directly on the medium or as a label attached to it. Alternatively, the media can be stored in marked containers.

SSI records may also be stored electronically on thumb drives. FTA strongly recommends that SSI on thumb drives be password-protected or encrypted. However, the thumb drives should not have any SSI marking on them.

7. Accessing SSI

Access to SSI records must be controlled to prevent unintended disclosure.[15] Restricting access to SSI means allowing only covered persons with a "need to know" to access them.

Need to know

Only persons with a "need to know" may access SSI. Regulations at 49 CFR §15.11 and §1520.11 describe "need to know" in relation to a person who needs access to SSI in order to:[16]

- Perform official duties, for example, pursuant to a contract or grant.
- Carry out, or supervise or manage persons who are carrying out, DHS- or DOT-approved, accepted, funded, recommended, or directed transportation security activities, or complete training to carry out such activities.
- Provide technical or legal advice to a "covered" person regarding transportation-security federal legal or regulatory requirements or in connection with a judicial or administrative proceeding regarding these requirements.

Because having a need to know is the only way in which an employee, contractor, or vendor can gain access to SSI, transit agencies should define their "need to know" requirements as a matter of policy to assure that all persons can access the information they need to perform their jobs.

Covered person

As defined in 49 CFR §15.3 and §1520.3, a "covered person" is "any organization, entity, individual, or other person described in [§15.7 or §1520.7]. In the case of an individual, the term *covered person* includes any individual applying for employment in a position that would be a covered person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. *Covered person* includes a person applying for certification or other form of approval that, if granted, would make the person a covered person as described in [§15.7 or §1520.7]."

Title 49 CFR §15.7 and §1520.7 list 13 types of "persons subject to the requirements of" or "covered" under these regulations: At this time, only the four types below apply to transit agency personnel:[17]

- Persons who have access to SSI
- Persons employed by, contracted to, or acting for a covered person, including a grantee of DHS or DOT, and persons formerly in such a position

[15] SSI is protected from public disclosure under FOIA, and, by law, must not be disclosed, except as provided in 49 CFR Parts 15 and 1520.
[16] For a complete listing, see 49 CFR §15.11 or §1520.11
[17] For complete text, see 49 CFR §15.7 or §1520.7

- Persons for whom a vulnerability assessment has been directed, created, held, funded, or approved by the DOT, DHS, or who have prepared a vulnerability assessment that will be provided to either agency in support of a Federal security program

- Persons receiving SSI.

8. Types of Access

Routine access

Routine access refers to the use and exchange of SSI by transit agency employees, contractors, vendors, and suppliers during the normal conduct of transit agency business. Transit agencies must assure that only persons with a need to know have access to SSI records. Covered persons, either originators or holders/recipients of the SSI, may grant routine access to other persons with a need to know by giving them the SSI. The SSI recipients then become covered persons for that information.

Contractors, vendors, and suppliers may need access to SSI such as facility security blueprints, for example, during the bidding process for capital projects. Transit agencies should establish rules for the dissemination of SSI to contractors. Options for transit agencies to control SSI needed by contractors, vendors, and suppliers include:

- *Qualified vendors list.* Transit agency procurement and legal departments can prequalify contractors, vendors, and suppliers to bid on contracts potentially involving SSI. Prequalifying contractors allows transit agencies time to investigate the contractors' business practices and history. Prequalification can also include nondisclosure agreements covering SSI records.

- *Secure locations.* Transit agencies can provide secure locations where contractors can access the SSI they need. These locations may be provided for on-site contractors as well as for contractors bidding on new work.

- *Contractual requirements.* Transit agency procurement and legal departments can assure that contracts contain terms and conditions for handling SSI, including use, storage, reproduction, dissemination, and return, both on and off of transit property.

Special access

Persons who do not have routine access to transit agency SSI records may be granted special access to specific SSI. For example, transit agencies might be requested to share specific SSI records as part of litigation. However, under the DHS Appropriations Act of 2007,[18] only TSA has the authority to share specific SSI with civil litigants.

Persons requesting special access must specify the SSI that they need to view. Transit agencies' legal departments should transmit all SSI provided under special access. Prior to doing so, the transit agencies should assure that the persons receiving the SSI are aware of the requirements for controlling it.

Unauthorized disclosure

Occasionally, transit agencies may experience unauthorized disclosure of SSI. Agencies need a policy and procedures for handling this loss of control, including appropriate disciplinary action.

[18] Public Law No. 109-295 (October 4, 2006).

Transit agency security organizations are most likely to receive reports of unauthorized disclosure. However, other departments, such as legal, IT, and engineering, may also receive them. Transit agencies should document and investigate all potential unauthorized disclosures and take appropriate actions.

The individuals or committees selected to categorize information as SSI should monitor potential unauthorized disclosures. If SSI is disclosed inappropriately, the individuals or committees should review the circumstances, assess potential damage, and address the need for changes in transit agency policies or procedures.

9. Controlling SSI

Transit agencies must control SSI during storage, use, reproduction, transmittal, and destruction. Appendix B provides TSA's "Sensitive Security Information Stakeholder Best Practices Quick Reference Guide." This guidance document, available through TSA, is consistent with TSA's stakeholder guide.

Storage

As needed, transit agencies may create one or many storage areas for SSI. For example, to facilitate daily business, each department or person may have a designated storage area for paper SSI. If possible, the owner or originator of the SSI should store it. For example, the engineering department should store engineering drawings categorized as SSI.

Not everyone who works at a transit agency has a "need to know" SSI. To preclude unauthorized access, SSI records should be stored in cabinets or rooms that can be locked unless the records are under direct supervision (that is, someone is working on them). If rooms are not locked or otherwise controlled, SSI should be stored in locked receptacles, such as file cabinets or desks.

SSI in electronic form on personal computers (PCs), floppy disks, CDs, DVD, tapes, or other electronic media should be password protected. If electronically stored SSI can be accessed remotely, it should be protected with a firewall, a virtual private network (VPN), or another secure connection.

Use

During use, SSI records should not be left out in the open. For example, if a person using paper SSI records must temporarily leave the area of use, he or she may protect the SSI by storing the records in a locked drawer. In addition, persons with knowledge of SSI should maintain vigilance when discussing SSI in meetings, on the telephone, or via radio. SSI should not be discussed in public conveyances or other locations that permit interception by unauthorized individuals.

Reproduction

SSI records may be reproduced only to the extent necessary to carry out transit agency business. Reproduced SSI must be marked and protected in the same manner as the original SSI. For example, persons photocopying paper SSI should make only the minimum number of copies needed. Copy machine malfunctions should be cleared and all paper paths checked for SSI. Excess paper containing SSI should be shredded.

Transmission

SSI can be sent to "known" persons, addresses, or locations on the basis of the receiver's "need to know." However, persons sending SSI must assure against unauthorized disclosure.

Within a transit agency, paper or electronic SSI, such as floppy disks and CDs, may be sent through interoffice mail with use of a standard internal distribution envelope. In addition, the sender may hand-carry the SSI to another person or location.

Sending paper or electronic SSI records outside of the transit agency requires packaging in a single, opaque envelope or wrapping. The sender may use any mail method or courier service to transmit the information, as well as any commercial carrier. In addition, the sender may hand carry the SSI (for example, in a purse or briefcase) as long as he/she can control access to it.

Transmission of SSI by telecommunications, such as telephone, facsimile, Internet, or e-mail, requires a "known" recipient with a "need to know" the SSI. E-mail attachments containing SSI should be encrypted or password-protected, and the key or password should be provided separately.

Return

Transit agencies need procedures for the return of SSI when it is no longer required by employees or contractors. For employees leaving a transit agency, human resource and legal departments should assure the return of SSI and should brief the exiting employees on their obligation not to disclose SSI. Similarly, employees who transfer to new positions should return SSI records that they no longer need.

Transit agencies should also require contractors, vendors, and suppliers to return SSI at the termination of their contracts or whenever it is no longer needed.

Destruction

Paper SSI must be destroyed using a method that precludes its recognition or reconstruction. FTA recommends, but does not require, that transit agencies use commercially available 'cross-cut' shredders that shred paper into pieces no bigger than one-half inch on a side. Transit agencies may designate other methods of destruction for both paper and other forms of SSI.

FTA also recommends, but does not require, that transit agencies develop an internal audit program or other documented, formal self-inspection method to assure that procedures for controlling SSI are effective. Audits or inspections may be done at intervals consistent with the agencies' risk-management principles.

10. Training

All transit agency employees who may create, receive, or use SSI should receive training on how to identify, handle, and protect it. In addition, SSI awareness training should be included in all new employee and refresher training. Contractors, vendors, and suppliers who may need access to SSI as part of their work should also be trained, either by the transit agencies or through their own companies.

Appendix A: Sample Front and Back Cover Pages for SSI

EXAMPLE

Front and Back Cover Page for Marking SSI Materials

SENSITIVE SECURITY INFORMATION

Transit Agency Name or Transit Agency Department Name

If this document/information is found, please deliver to appropriate department or position as soon as possible.

Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Appendix B: TSA's Sensitive Security Information Stakeholder Best Practices Quick Reference Guide

What is SSI?

Sensitive Security Information (SSI) is information that, if publicly released, would be detrimental to transportation security as defined by Federal regulation 49 C.F.R. part 1520.

Although SSI is not classified information, there are specific procedures for recognizing, marking, protecting, safely sharing, and destroying SSI.

Recognizing SSI

The following information constitutes SSI:

1. Security programs and contingency plans
2. Security directives
3. Information circulars
4. Performance specifications
5. Vulnerability assessments
6. Security inspections or investigative information
7. Threat information
8. Security measures
9. Security screening information
10. Security training materials
11. Identifying information of certain transportation security personnel
12. Critical infrastructure asset information
13. Systems security information
14. Confidential business information
15. Research and development
16. Other information as determined in writing by the TSA Administrator

The purpose of this brochure is to provide transportation security stakeholders with best practices for handling SSI. Best practices are not to be construed as legally binding requirements of, or official implementing guidance for, the SSI regulation.

The SSI Office

TSA's Sensitive Security Information (SSI) Office:

- ✓ Develops SSI guidance, policies, and procedures to help others appropriately recognize and handle SSI.
- ✓ Analyzes and reviews records for SSI content.
- ✓ Trains TSA employees, clients, and stakeholders in identifying, handling, marking, sharing, storing, transmitting, and destroying SSI.
- ✓ Coordinates with stakeholders, other governmental agencies, and Congress on SSI-related issues.

www.tsa.gov

For more information:

Phone: (571) 227-3513
Fax: (571) 227-2945
SSI@dhs.gov

Sensitive Security Information

✓Stakeholder Best Practices Quick Reference Guide

Transportation Security Administration

Safely Sharing Information

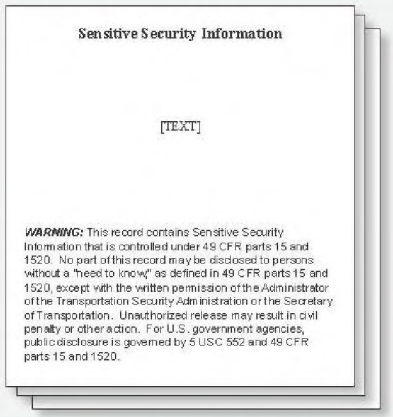
SSI Requirements

The SSI regulation mandates specific and general requirements for handling and protecting SSI.

You Must – Lock-up All SSI
When not in physical possession, store SSI in a secure container such as a locked file cabinet or drawer.

You Must – When No Longer Needed, Destroy SSI
Destruction of SSI must be complete to preclude recognition or reconstruction of the information.

You Must – Mark SSI
The regulation requires that when only a small portion of a paper document contains SSI, every page of the document must be marked with the SSI header and footer shown below.



When Combining SSI With Other Sensitive But Unclassified (SBU) Information, the document must be marked as SSI. SSI extracted from SSI documents requires the new document to be marked and protected as SSI.

Best Practices Guide

Reasonable Steps Must be Taken to Safeguard SSI. While the regulation does not define reasonable steps, the TSA SSI Office offers these best practices as examples of reasonable steps:

- ✓ **Electronic Presentations** (e.g., PowerPoint) should be marked with the SSI header on all pages and the SSI footer on the first and last pages of the presentation.
- ✓ **Spreadsheets** should be marked with the SSI header on every page and the SSI footer on every page or at the end of the document.
- ✓ **Video and Audio** should be marked with the SSI header and footer on the protective cover when able and the header and footer should be shown and/or read at the beginning and end of the program.
- ✓ **CDs and DVDs** should be encrypted or password-protected and the header and footer should be affixed to the CD or DVD.
- ✓ **Portable Drives** including "flash" or "thumb" drives should not themselves be marked, but the drive itself should be encrypted or all documents stored should be password-protected.
- ✓ **When Leaving Your Computer or Desk** you must lock up all SSI and should lock or turn off your computer.
- ✓ **Taking SSI Home** is not recommended, but if necessary, get permission from a supervisor and lock up all SSI at home.
- ✓ **Discussing SSI Over Cellular Telephones** should be done carefully to prevent eavesdropping. Land lines in non-public locations are more secure than cellular telephones.
- ✓ **Email** should not contain SSI in the body of the email. SSI should be emailed in a password-protected attachment. Passwords should be sent separately with no subject line or shared either in person or via telephone.
- ✓ **Passwords for SSI Documents** should contain at least 8 characters, have at least one upper-cased and one lower-cased letter, contain at least one number, and not be a word in the dictionary.
- ✓ **Faxing of SSI** should be done by first verifying the fax number and that the intended recipient will be available to retrieve the SSI once faxed.
- ✓ **SSI Should Be Mailed** by U.S. First Class mail or other traceable delivery service using an opaque envelope or wrapping and the outside wrapping should not be marked as SSI.
- ✓ **Interoffice Mail** should be sent using an unmarked, opaque, sealed envelope so that the SSI cannot be read through the envelope.
- ✓ **SSI Stored on Network Folders** should either require a password to open or the network should limit access to the folder.
- ✓ **Destroying SSI** should be done using a cross-cut shredder which produces particles that are 1½ inch by 3/16 inch or smaller.

Sensitive Security Information Office

Safely Sharing Information